National Infrastructure Protection Center
CyberNotes

Issue #2002-19 *September 23, 2002*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between September 6 and between September 19, 2002. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Apple[1]	MacOS X 10.2	MacOS X 10.2 (Jaguar)	A vulnerability exists in NetInfo Manager because privileges are not sufficiently dropped prior to execution, which could let a malicious user obtain root access.	No workaround or patch available at time of publishing.	NetInfo Manager Unauthorized Access	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.

[1] Bugtraq, September 13, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Apple[2]	Windows NT 4.0/2000, XP	Quicktime ActiveX Component 5.0.2	A buffer overflow vulnerability exists due to the way the component handles the "pluginspage" field when it is parsed from a malicious remote or local HTML page, which could let a malicious user execute arbitrary code.	Upgrade available at: http://www.apple.com/quicktime/.	Quicktime ActiveX Component Buffer Overflow CVE Name: CAN-2002-0376	**High**	Bug discussed in newsgroups and websites.
atftp[3]	Unix	atftp 0.5, 0.6	A buffer overflow vulnerability exists in the 'get file' parameter due to insufficient bounds checking of user input to the command line parameter (-g), which could let a malicious user execute arbitrary instructions.	No workaround or patch available at time of publishing.	ATFTP Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Avaya[4]	Multiple	IP Office Firmware 1.0	A Denial of Service vulnerability exists when malformed packets are handled on user and administrative application ports.	No workaround or patch available at time of publishing.	IP Office Malformed Packets Denial of Service	Low	Bug discussed in newsgroups and websites.
Cerulean Studios[5]	Windows	Trillian 0.73, 0.74	A buffer overflow vulnerability exists when 'PRIVMSG' commands are processed that contain an overly large sender name, which could let a malicious user cause a Denial of Service and possibly execute arbitrary code.	No workaround or patch available at time of publishing.	Trillian IRC PRIVMSG Buffer Overflow	Low/**High** **(High if arbitrary code is executed)**	Bug discussed in newsgroups and websites. Exploit script has been published.
Cerulean Studios[6]	Windows 95/98/ME NT 4.0/2000	Trillian 0.73, 0.725, 0.6351	A vulnerability exists because weak encryption is used to store saved authentication credentials, which could let a malicious user obtain unauthorized access.	No workaround or patch available at time of publishing.	Trillian Weak Password Encryption	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Cerulean Studios[7]	Windows 95/98/ME/ NT 4.0/2000	Trillian 0.73, 0.74, 0.725, 0.6351	A buffer overflow vulnerability exists in the 'ident' server when a malformed request is received that is 418 bytes or more, which could let a malicious user cause a Denial of Service or execute arbitrary code.	No workaround or patch available at time of publishing.	Trillian Identd Buffer Overflow	Low/**High** **(High if arbitrary code is executed)**	Bug discussed in newsgroups and websites. Exploit script has been published.

[2] @stake Inc. Security Advisory, a091002-1, September 10, 2002.
[3] Netric Security Team, September 19, 2002.
[4] SecurityFocus, September 13, 2002.
[5] NTBugtraq, September 19, 2002.
[6] Bugtraq, September 9, 2002.
[7] Bugtraq, September 18, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Check Point Software[8]	Multiple	Firewall-1 4.1, 4.1 SP1-SP6, Next Generation, Next Generation FP1&FP2	A vulnerability exists because the contents of sessions are not properly checked when passed through the HTTP proxy server, which could let a remote malicious pass protocols through the system that violate the security policy.	No workaround or patch available at time of publishing.	Firewall-1 HTTP Proxy Server	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Cisco Systems[9]	Multiple	IP Phone 7960	Several vulnerabilities exist in the TFTP (Trivial File Transfer Protocol) because authentication is not required to download firmware images and configuration files, which could let a malicious user install arbitrary firmware; and a vulnerability exists when TFTP is conducted over UDP because authentication is not provided, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	IP Phone 7960 Unsigned Content Weakness	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Cisco Systems[10]	Mac OS	VPN 5000 Client for Mac OS 5.1.2, Mac OS 5.2.1	A vulnerability exists when the “Default Connection” is saved in the resource fork of the preference file because the entire contents of the data structure that represents the "Default Connection" are saved, which could let a malicious user obtain password information.	The procedure to upgrade to the fixed software version is detailed at: http://www.cisco.com/univercd/cc/td/doc/product/aggr/vpn5000/client/.	Mac OS VPN 5000 Client Password Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited using any tool that allows users to view resource forks.
Cisco Systems[11]	Unix	VPN 5000 Client for Linux 5.2.6, VPN 5000 Client for Solaris 5.2.7	Two buffer overflow vulnerabilities exist: a buffer overflow vulnerability exists in the 'close_tunnel' binary, which could let a malicious user obtain root privileges; and a buffer overflow vulnerability exists in the 'open_tunnel' binary, which could let a malicious user obtain root privileges.	The procedure to upgrade to the fixed software version is detailed at: http://www.cisco.com/univercd/cc/td/doc/product/aggr/vpn5000/client/.	VPN 5000 Client Buffer Overflow Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.

[8] SecurityFocus, September 18, 2002.
[9] SecurityFocus, September 19, 2002.
[10] Cisco Security Advisory, September 18, 2002.
[11] Cisco Security Advisory, September 18, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Compaq Computer Corpora-tion[12]	Unix	Tru64 4.0g PK3 (BL17), 4.0g, 4.0f PK7 (BL18), 4.0f PK6 (BL17), 4.0f, 5.0a PK3 (BL17), 5.0a	A Denial of Service vulnerability exists because predictable initial TCP sequence numbers (ISNs) are used.	Patches available at: http://ftp.support.compaq.com/patches/public/unix/v4.0g/ http://ftp.support.compaq.com/patches/public/unix/v4.0f/ http://ftp.support.compaq.com/patches/public/unix/v5.0a/	HP Tru64 Initial Random TCP Sequence Number Denial of Service	Low	Bug discussed in newsgroups and websites.
Compaq Computer Corpora-tion[13]	Unix	Tru64 4.0g PK3 (BL17), 4.0g, 4.0f PK7 (BL18), 4.0f PK6 (BL17), 4.0f, 5.0f, 5.0a PK3 (BL17), 5.0a, 5.0 PK4 (BL18), 5.0 PK4 (BL17), 5.0, 5.1a PK1 (BL1), 5.1a, 5.1 PK4 (BL18), 5.1 PK3 (BL17), 5.1	A vulnerability exists in the Address Resolution Protocol (ARP) implementation, which could let a remote malicious system "take over packets destined for another host," and under certain circumstances cause a Denial of Service.	Patches available at: http://ftp.support.compaq.com/patches/public/unix/v4.0g/ http://ftp.support.compaq.com/patches/public/unix/v4.0f/ http://ftp.support.compaq.com/patches/public/unix/v5.0a/	Tru64 Address Resolution Protocol	Low/ Medium (Low if a Denial of Service)	Bug discussed in newsgroups and websites.
DB4Web [14]	Multiple	DB4Web 3.4, 3.6	A Directory Traversal vulnerability exists when a maliciously crafted query is passed to the application due to insufficient user input validation, which could let a malicious user obtain sensitive information.	Patch available at: http://www.db4web.de/download/homepage/hotfix/	DB4Web Directory Traversal	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
DB4Web [15]	Multiple	DB4Web 3.4, 3.6	A vulnerability exists when a request is made for a specially crafted URL, which could let a malicious user initiate a TCP connect to a remote IP address and arbitrary port.	No workaround or patch available at time of publishing.	DB4Web Connection Proxy	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.

[12] Hewlett Packard Security Advisory, September 10, 2002.
[13] Hewlett Packard Security Advisory, SSRT-547, September 11, 2002.
[14] Guardeonic Solutions AG Security Advisory #01-2002, September 17, 2002.
[15] Guardeonic Solutions AG Security Advisory #02-2002, September 17, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Digital[16]	Unix	Digital OSF/1 3.0, 3.0B, 3.2G, 3.2F, 3.2, 3.2 DE1&2, 3.2B-3.2D, UNIX 3.0, 3.2 G	A buffer overflow vulnerability exists in the 'UUCP' utility, which could let a malicious user execute arbitrary code.	Upgrade to one of the later versions of Tru64.	Tru64 UUCP Local Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Digital[17]	Unix	OSF/1 3.0, 3.0 B, 3.2G, 3.2F, 3.2 DE1&2, 3.2, 3.2 B-D, 4.0, Ultrix 3.0	A buffer overflow vulnerability exists in the 'inc' mail incorporation utility, which could let a malicious user execute arbitrary commands as the root user.	Upgrade to one of the later versions of Tru64.	Tru64 Inc Local Buffer Overflow CVE Name: CAN-2002-1128	**High**	Bug discussed in newsgroups and websites.
Enterasys [18]	Multiple	Smart Switch SSR8000 E8.3.0.4, SSR8000 E8.2.0.0	A remote Denial of Service vulnerability exists when a malicious user performs a port scan several times on ports 15077 and 15078.	Upgrade available at: http://www.enterasys.com/download/download.cgi?lib=ssr	SSR8000 SmartSwitch Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
FreeBSD [19, 20]	Unix	FreeBSD 4.2-4.6	Vulnerabilities exists in the 'asmon', 'ascpu', 'bubblemon', 'wmmon', and 'wmnet2' ports due to a leakage of open file descriptors, which could let a malicious user obtain root privileges.	Patch available at: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-02:39/libkvm.patch	FreeBSD Ports libkvm Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Gabriele Bartolini[21]	Unix	ht://Check 1.1	A Cross-Site Scripting vulnerability exists because HTML tags are not properly filtered before displaying Web server's 'Server:' headers after scanning the server for dead links, which could let a remote malicious user execute arbitrary HTML or script code.	No workaround or patch available at time of publishing.	ht://Check Web Header Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.

[16] iDEFENSE Security Advisory 09.18.2002, September 18, 2002.
[17] iDEFENSE Security Advisory 09.18.2002, September 18, 2002.
[18] ISS Security Alert Summary AS02-37, September 16, 2002.
[19] iDEFENSE Security Advisory, September 16, 2002.
[20] FreeBSD Security Advisory, FreeBSD-SA-02:39, September 16, 2002.
[21] Securiteam, September 12, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Hewlett Packard Systems[22]	Unix	Compaq Tru64 4.0g, 4.0g PK3 (BL17), 4.0f, 4.0 f PK7 (BL18), 4.0 f PK6 (BL17), 5.0a, 5.0 a PK3 (BL17), 5.0, 5.0 PK4 (BL18), 5.0 PK4 (BL17), 5.1a, 5.1a PK2 (BL2), 5.1a PK1 (BL1), 5.1, 5.1 PK5 (BL19), 5.1 PK4 (BL18), 5.1 PK3 (BL17); Digital OSF/1 3.0, 3.0 B, 3.2, 3.2 G, 3.2 F, 3.2 DE1&2, 3.2 B-3.2D	A buffer overflow vulnerability exists in the 'dxterm' utility due to insufficient checking of command line input supplied via the "-xrm" parameter, which could let a malicious user exploit arbitrary code and obtain root privileges.	Upgrades available at: ftp://ftp1.support.compaq.com/public/unix/	Tru64/OSF1 DXTerm Buffer Overflow CVE Name: CAN-2002-1129	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
IBM[23]	Windows 2000	Websphere Application Server 4.0.3	A buffer overflow vulnerability exists due to improper bounds checking when HTTP requests are received, which could let a malicious user cause a Denial of Service.	Patch available at: http://www-1.ibm.com/support/docview.wss?rs=180&context=SSEQTP&q=PQ62144&uid=swg24001610	WebSphere Large HTTP Header Denial of Service	Low	Bug discussed in newsgroups and websites.
Internet Security Systems[24]	Multiple	Internet Scanner 6.2.1	A buffer overflow vulnerability exists because the license banner HTTP check performed does not check the length of the data returned by the web server being tested, which could let a malicious user execute arbitrary code.	Upgrade available at: http://www.iss.net/download/	Internet Scanner HTTP Banner Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

[22] iDEFENSE Security Advisory 09.18.2002, September 18, 2002.
[23] KPMG-2002035, September 19, 2002.
[24] Foundstone Research Labs Advisory, 091802-ISSC, September 18, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Joseph Allen[25]	Unix	joe 2.8, 2.9, 2.9.1, 2.9.2, 2.9.4-2.9.7	A vulnerability exists due to the way backup files are handled, which could let a malicious user create an arbitrary copy of the root owned suid file.	No workaround or patch available at time of publishing.	Joe Text Editor Backup SetUID Executable Editing Permission Elevation	**High**	Bug discussed in newsgroups and websites.
KDE[26]	Unix	KDE 3.0-3.0.2	A vulnerability exists in the Konquerer component because the presence of secure flags in cookies is not properly acknowledged, which could let a malicious user intercept "secure" cookie-based authentication credentials.	Upgrade available at: ftp://ftp.kde.org/pub/kde/security_patches	KDE Secure Cookie Exposure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
KDE[27]	Unix	KDE 2.1-2.2.2, 3.0, 3.0.2	A Denial of Service vulnerability exists when overly wide images are processed.	Upgrade available at: http://www.kde.org/download.html	KDE Konqueror Oversized Image Width Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
KDE-[28, 29]	Unix	KDE 2.2.2, 3.0, 3.0.1-3.0.3, Konqueror 2.2.2, 3.0, 3.0.1-3.0.3	A vulnerability exists because the domain of sub-frames or sub-iframes is not set properly, which could let a malicious user execute arbitrary script code.	**KDE:** http://download.kde.org/stable/3.0.3 **Debian:** http://security.debian.org/pool/updates/main/k/kdelibs/ **Conectiva:** ftp://atualizacoes.conectiva.com.br/	KDE Konqueror Sub-Frames Script Execution	**High**	Bug discussed in newsgroups and websites.
KTH[30]	Unix	Heimdal 0.4 a-0.4 e	Several vulnerabilities exist: a vulnerability exists because the Kerberos Forwarding Daemon sends user and file information without integrity protection, which could let a malicious user overwrite any file and possibly exploit root; and a vulnerability exists because information sent from a client to a server is not properly checked for the termination of strings, which could let a malicious user exploit root.	Update available at: ftp://ftp.pdc.kth.se/pub/heimdal/src/heimdal-0.5.tar.gz	Kerberos Forwarding Daemon File Overwriting	Medium/ **High** **(High if root is exploited)**	Bug discussed in newsgroups and websites.

[25] Bugtraq, September 17, 2002.
[26] KDE Security Advisory, September 10, 2002.
[27] sp00fed packet advisory #2, September 15, 2002.
[28] KDE Security Advisory, September 10, 2002.
[29] Debian Security Advisory, DSA 167-1, September 16, 2002.
[30] NetBSD Security Advisory 2002-018, September 17, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Lycos[31]	Multiple	htmlGEAR guest GEAR	A vulnerability exists because HTML is not sanitized from CSS (Cascading Style-Sheets) elements in guestbook fields, which could let a malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	guestGear CSS HTML Injection	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft [32]	Windows	JVM 1.1	Numerous vulnerabilities exist in the Java Virtual Machine (JVM) implementation which could let a malicious user obtain file access on the viewer's system, allow access to other resources, or allow execution of arbitrary code. Most of these vulnerabilities are related to Microsoft-specific native methods used within the various classes.	No workaround or patch available at time of publishing.	Multiple JVM Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
Microsoft [33]	Windows 95/98/NT 4.0/2000	Outlook Express 5.01, 5.0, 5.5, 6.0	A Denial of Service vulnerability exists when a HTML e-mail is decoded if a <A HREF> link is longer than 4095 characters.	No workaround or patch available at time of publishing.	Outlook Express Link Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept script has been published.
Microsoft [34]	Windows 95/98/NT 3.51/4.0/ 2000	Virtual Machine 2000 Series, 3000 Series, 3100 Series, 3188, 3200 Series, 3300 Series, 3802 Series, 3805 Series	Multiple vulnerabilities exist: a vulnerability exists in the Java Database Connectivity (JDBC) classes due to flaw in the way the classes vet a request to load and execute a DLL, which could let a remote malicious user load and execute any DLL on the user's system; a vulnerability exists in the JDBC classes because certain functions in the classes don't correctly validate handles that are provided as input, which could let a malicious user cause a Denial of Service and possible execute arbitrary code; and a vulnerability exists that involves a Java class that provides support for use of XML methods due to a flaw in the design, which could let a malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-052.asp	Virtual Machine Multiple Vulnerabilities CVE Names: CAN-2002-0865, CAN-2002-0866, CAN-2002-0867	Low/**High** **(High if arbitrary code is executed)**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.

[31] Securiteam, September 16, 2002.
[32] Bugtraq, September 9, 2002.
[33] Bugtraq, September 9, 2002.
[34] Microsoft Security Bulletin, MS02-052, September 18, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [35]	Windows NT 4.0/2000, XP	Windows 2000 Advanced Server, Windows 2000 Advanced Server SP1-3, Datacenter Server, Datacenter Server SP1-3, 2000 Profes-sional, 2000 Profes-sional SP1-3, 2000 Server, 2000 Server SP1-3, Terminal Services, Terminal Services SP1-3, NT Terminal Server 4.0, Terminal Server 4.0 SP1-6a, XP 64-bit Edition, XP 64-bit Edition SP1, XP Home, XP Home SP1, XP Profes-sional, XP Profes-sional SP1	Two vulnerabilities exist: a vulnerability exists due to how session encryption is implemented in certain versions of the Remote Desktop Protocol (RDP), which could let a malicious user obtain sensitive information; and a remote Denial of Service vulnerability exists due to the way the RDP implementation in Windows XP handles malformed data packets.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-051.asp	Microsoft Windows RDP Vulnerabilities CVE Names: CAN-2002-0863, CAN-2002-0864	Low/ Medium (Medium if sensitive informa-tion is obtained)	Bug discussed in newsgroups and websites. There is no exploit code required for the Encrypted RDP vulnerability. Exploit has been published for the XP Denial of Service vulnerability. Vulnerability has appeared in the press and other public media.

[35] Microsoft Security Bulletin, MS02-051, September 18, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [36]	Windows NT 4.0/2000, XP	Windows 2000 Advanced Server, Windows 2000 Advanced Server SP1-3, Datacenter Server, Datacenter Server SP1-3, 2000 Profes-sional, 2000 Profes-sional SP1-3, 2000 Server, 2000 Server SP1-3, Terminal Services, Terminal Services SP1-3, NT Terminal Server 4.0, Terminal Server 4.0 SP1-6a, XP 64-bit Edition, XP 64-bit Edition SP1, XP Home, XP Home SP1, XP Profes-sional, XP Profes-sional SP1	A vulnerability exists when a 16-bit application is executed for an 16-bit program that is already running, which could let a malicious user execute unauthorized programs.	No workaround or patch available at time of publishing.	Windows 2000/NT/XP 16-bit Application Permission Bypass	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[36] Abtrusion Security, September 18, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [37]	Windows 95/98/ME/ NT 4.0/2000	Internet Explorer 5.0, 5.0 for Windows 95/98/ NT 4.0/2000, 5.0.1, 5.0.1 SP1&2, 5.0.1 for Windows 95/98/NT 4.0/2000, 5.5, 5.5 SP1&2, 5.5 preview, 6.0	A vulnerability exists because it is possible for a parent window to set the URL of frames or iframes within a child window regardless of the domain or Security Zone, which could let a remote malicious user execute arbitrary script code.	Temporary workaround: Disable scripting	Internet Explorer IFrame/Frame Cross-Site/Zone Script Execution	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published. Vulnerability has appeared in the press and other public media.
Microsoft [38]	Windows NT 4.0/2000	NetMeeting 3.0.1 4.4.3385	A vulnerability exists in the RDS module because the remote session can be hijacked at the host, which could let a malicious user with physical access to the host system obtain local or network administration privileges.	No workaround or patch available at time of publishing.	Netmeeting Local Session Hijacking	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Mozilla[39]	Windows 95/98/ME/ NT 4.0/2000, XP, MacOS 9.0/ 9.0.4/ 9.1/ 9.2/ 9.2.1/9.2.2, MacOS X 10.x, BeOS 5.0, Unix	Mozilla Browser 0.9.3-0.9.9, 1.0, 1.0.1, 1.1	A vulnerability exists in the implementation of the JavaScript 'onUnload' event handler because requests that the handler launches have the wrong referer, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Mozilla OnUnload Referer Information Leakage	Medium	Bug discussed in newsgroups and websites. Proof of Concept has been published. Vulnerability has appeared in the press and other public media.
Multiple Vendors[40]	Windows 95/98/ME/ NT 4.0/2000, XP, MacOS 9.0/9.0.4/ 9.1/9.2/9.2.1 MacOS X 10.x, Unix, BeOS 5.0	Mozilla Browser 0.9.5-0.9.9, 1.0; Netscape 6.2-6.2.3; Opera Software Opera Web Browser 5.12. 6.0, 6.0.1	A vulnerability exists when GIF image files are handled that have the width field set to zero, which could let a malicious user cause a Denial of Service or potentially execute arbitrary code.	**Mozilla:** http://www.mozilla.org/releases/ **Netscape:** http://channels.netscape.com/ns/browsers/download.jsp	Multiple Vendor Zero Width GIF Image Files	Low/**High** **(High if arbitrary code is executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.

[37] GreyMagic Security Advisory, GM#010-IE, September 9, 2002.
[38] Securiteam, September 18, 2002.
[39] Securiteam, September 12, 2002.
[40] Securiteam, September 8, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[41]	Windows NT 3.5/ 3.5.1/4.0	GFI Mail Security for Exchange/SMTP 7.2; Network Associates WebShield SMTP 4.0.5, 4.5, 4.5.44, 4.5.74.0; Roaring Penguin Software CanIt 1.2, MIME Defang 2.14, 2.20; Trend Micro InterScan VirusWall for Windows NT 3.5, 3.51, 3.52,	A vulnerability exits due to improper handling of messages that have been sent using the 'Message Fragmentation and Re-assembly' option, which could let a remote malicious user bypass content filtering and deliver viruses, Trojan's, or other malicious file types to a vulnerable mail client.	**Roaring Penguin Software:** http://www.roaringpenguin.com/mimedefang/MIME-tools-5.411a-RP-Patched.tar.gz **TrendMicro:** ftp://ftp-download.trendmicro.com.ph/Gateway/ISNT/3.52/Hotfix_build1494_v352_Smtp_case6593.zip **GFI:** GFI has updated MailSecurity for Exchange/SMTP version 7.2. Users should contact the vendor for updated software.	Multiple Vendor Email Message Fragmentation SMTP Filter Bypass CVE Name: CAN-2002-1121	**High**	Bug discussed in newsgroups and websites. There is no exploit code required. Vulnerability has appeared in the press and other public media.
NetBSD[42]	Unix	NetBSD 1.4, 1.4 x86, SPARC, arm32, Alpha, 1.4.1, 1.4.1 x86, 1 SPARC, sh3, arm32, Alpha, 1.4.2, 1.4.2 x86, SPARC, arm32, Alpha, 1.4.3, 1.5, 1.5 x86, sh3, 1.5.1-1.5.3, 1.6 beta	A buffer overflow vulnerability exists because repeated calls that are made to 'TIOSCTTY' will cause an internal buffer to be incremented indefinitely and overflow, which could let a malicious user cause a kernel panic or cause faulty terminal sessions.	Upgrade information available at: ftp://ftp.NetBSD.org/pub/NetBSD/security/advisories/NetBSD-SA2002-007.txt.asc	NetBSD Repeated TIOSCTTY IOCTL Buffer Overflow	Low	Bug discussed in newsgroups and websites.

[41] Securiteam, September 12, 2002.
[42] NetBSD Security Advisory, 2002-007, September 17, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
NetBSD[43]	Unix	NetBSD 1.4, 1.4 x86, SPARC, arm32, Alpha, 1.4.1, 1.4.1 x86, 1 SPARC, sh3, arm32, Alpha, 1.4.2, 1.4.2 x86, SPARC, arm32, Alpha, 1.4.3, 1.5, 1.5 x86, sh3, 1.5.1-1.5.3	A buffer overflow vulnerability exists in the setlocale() function in libc, which could let a malicious user obtain root access.	Upgrade information available at: ftp://ftp.NetBSD.org/pub/NetBSD/security/advisories/NetBSD-SA2002-012.txt.asc	NetBSD LibC SetLocale Buffer Overflow	High	Bug discussed in newsgroups and websites.
NetBSD[44]	Unix	NetBSD 1.4, 1.4 x86, SPARC, arm32, Alpha, 1.4.1, 1.4.1 x86, 1 SPARC, sh3, arm32, Alpha, 1.4.2, 1.4.2 x86, SPARC, arm32, Alpha, 1.4.3, 1.5, 1.5 x86, sh3, 1.5.1-1.5.3	A buffer overflow vulnerability exists in the IPv4 multicast-related tools mrinfo(1) and mtrace(1), and the PPP daemon pppd(8) due to improper boundary checking when the FD_SET() operation is performed, which could let a malicious user obtain root privileges.	Upgrade information available at: ftp://ftp.NetBSD.org/pub/NetBSD/security/advisories/NetBSD-SA2002-014.txt.asc	NetBSD IPv4 Multicast Tools Buffer Overflow	High	Bug discussed in newsgroups and websites.
NetGear[45]	Multiple	FM114P	A vulnerability exists because host and domain names are note resolved by default, which could let a malicious user access a restricted site.	No workaround or patch available at time of publishing.	NetGear FM114P Prosafe URL Filter Bypassing	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Netris[46]	Unix	Netris 0.3-0.5	A remote Denial of Service vulnerability exists due to a buffer overflow when a malicious user sends an overly long string to the server.	No workaround or patch available at time of publishing.	Netris Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.

[43] NetBSD Security Advisory 2002-012, September 17, 2002.
[44] NetBSD Security Advisory 2002-014, September 17, 2002.
[45] Bugtraq, September 7, 2002.
[46] ISS Security Alert Summary AS02-37, September 16, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Netscreen [47]	Multiple	Netscreen-Remote Security Client 8.0, Remote VPN Client 8.0	A buffer overflow vulnerability exists when malformed IKE packets are sent to the client, which could let a remote malicious user cause a Denial of Service and possible execute arbitrary code.	Netscreen has stated that version 8.1 of the Netscreen-Remote VPN Client and Netscreen-Remote Security Client will be available on September 30, 2002, and can be downloadable via: http://www.netscreen.com/support/updates.html (login required)	Netscreen-Remote VPN Client IKE Packet Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
OpenSSL Project [48, 49, 50, 51, 52, 53, 54, 55, 56, 57] ***New Internet worm circulating that exploits the SSLv2 handshake vulnerability*** [58]	**Unix**	**OpenSSL 0.9.7 beta1&2**	**Multiple vulnerabilities exist: a buffer overflow vulnerability exists during the SSLv2 handshake process if a malformed key is used, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; a buffer overflow vulnerability exists during the SSLv3 handshake process if a large session ID is sent to the client during the handshake process, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; a buffer overflow vulnerability exists if Kerberos is enabled when a malformed key is sent during the SSLv3 handshake process, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; and multiple buffers overflow vulnerabilities exist in buffers that are used to hold ASCII representations of integers, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.**	**Contact your vendor for current updates or see CERT® Advisory CA-2002-23 located at: http://www.cert.org/advisories/CA-2002-23.html** **OpenSSL: http://www.openssl.org/news/** **Debian: http://security.debian.org/pool/updates/main/o/openssl/** **Trustix: http://www.trustix.net/pub/Trustix/updates/** **Mandrake: http://www.mandrakesecure.net/en/ftp.php** **Conectiva: ftp://atualizacoes.conectiva.com.br/** **Caldera: ftp://ftp.caldera.com/pub/security/OpenLinux/CSSA-2002-033.1.txt** **Engarde: http://ftp.engardelinux.org/pub/engarde/stable/updates/** **Oracle: http://otn.oracle.com/deploy/security/htdocs/opensslAlert.html** **Apple: http://docs.info.apple.com/article.html?artnum=120139**	**Multiple OpenSSL Vulnerabilities** **CVE Name: CAN-2002-0655, CAN-2002-0656, CAN-2002-0657**	**Low/High** **(High if arbitrary code can be executed)**	**Bug discussed in newsgroups and websites. Exploit script has been published.** ***Self-propagating malicious code circulating which exploits the SSLv2 handshake buffer overflow. This malicious code has been referred to as Apache/mod_ssl worm, linux.slapper. worm, and bugtraq.c worm.***

[47] NetScreen Security Advisory, September 6, 2002.
[48] CERT® Advisory CA-2002-23, July 30, 2002.
[49] Debian Security Advisory, DSA-136-1, July 30, 2002.
[50] Trustix Secure Linux Security Advisory, TSLSA-2002-0063, July 30, 2002.
[51] OpenPKG Security Advisory, OpenPKG-SA-2002.008, July 30, 2002.
[52] Gentoo Linux Security Announcement, July 30, 2002.
[53] Mandrake Linux Security Update Advisory, MDKSA-2002:046 1, August 6, 2002.
[54] SuSE Security Announcement, SuSE-SA:2002:027, July 30, 2002.
[55] Conectiva Linux Security Announcement, CLA-2002:513, July 31, 2002.
[56] Caldera International, Inc. Security Advisory, CSSA-2002-033.1, August 2, 2002.
[57] EnGarde Secure Linux Security Advisory, ESA-20020730-019, July 30, 2002.
[58] CERT® Advisory, CA-2002-27, September 17, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Opera Software[59]	Unix	Opera Web Browser 6.0.1 Linux	A Denial of Service vulnerability exists when overly wide images are processed.	Upgrade available at: http://www.opera.com/download/	Opera Oversized Image Width Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
PHP[60]	Unix	PHP 4.2.3	A vulnerability exists in the header function due to the way certain PHP scripts handle incoming URLs, which could let a malicious user execute arbitrary HTML and JavaScript code.	No workaround or patch available at time of publishing.	PHP Header Function Script Injection	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
PHP[61, 62]	MacOS X 10.x, Unix	PHP 3.0.14 – 3.0.18, 4.0.3-4.0.7, 4.1.0-4.1.2, 4.2.0-4.2.3	A vulnerability exists in the fopen(), file(), and other functions in PHP due to inadequate user input filtering, which could let a remote malicious user create fake HTTP headers by injecting CRLF combinations into HTTP headers using a specially-crafted URL request.	Update available at: http://cvs.php.net/diff.php/php4/ext/standard/url.c?r1=1.51&r2=1.52&ty=u&Horde=0 **Debian:** http://security.debian.org/pool/updates/main/p/php3/	PHP Function fopen() CRLF Injection	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
phpGB[63]	Unix	phpGB 1.1	A vulnerability exists because HTML tags are not checked when guestbook entries are generated, which could let a malicious user execute arbitrary HTML and script code.	Upgrade available at: http://www.walzl.net/michi/info.phtml	phpGB HTML Injection	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
phpGB[64]	Unix	phpGB 1.1, 1.2	A vulnerability exists in the 'savesettings.php' script due to inadequate authentication, which could let a malicious user bypass authentication and inject arbitrary code into the configuration file.	Upgrade available at: http://www.walzl.net/michi/info.phtml	phpGB PHP Code Injection	**High**	Bug discussed in newsgroups and websites. Proof of Concept has been published.
phpGB[65]	Unix	phpGB 1.1, 1.2, 1.3	A SQL injection vulnerability exists because the bulletin board relies on the PHP 'magic_quotes_gpc' directive to sanitize variables that are used in SQL queries, which could let a remote malicious user corrupt the database and obtain administrative guestbook privileges.	Upgrade available at: http://www.walzl.net/michi/info.phtml	phpGB SQL Injection	Medium/ **High** **(High if admnis-trative privileges are obtained)**	Bug discussed in newsgroups and websites. Proof of Concept has been published.

[59] sp00fed packet advisory #2, September 15, 2002.
[60] Securiteam, September 9, 2002.
[61] Securiteam, September 11, 2002.
[62] Debian Security Advisory, DSA 168-1, September 18, 2002.
[63] Bugtraq, September 9, 2002.
[64] Bugtraq, September 9, 2002.
[65] Bugtraq, September 9, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Planet DNS[66]	Window NT	PlanetWeb 1.14	A buffer overflow vulnerability exists when handling GET requests that are 1024 bytes or greater, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	PlanetWeb Long GET Request Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Purity[67]	Unix	Purity 1-9, 1-14, 1-15	Two buffer overflow vulnerabilities exist which could let a remote malicious user gain the privileges of the group games, which could then be used to perform limited actions on the vulnerable system.	**Debian:** http://security.debian.org/pool/updates/main/p/purity/	Purity Buffer Overflows	Medium	Bug discussed in newsgroups and websites.
Raxnet[68] ***Upgrades now available for the rrdtool 'graph' vulnera-bility[69]***	**Multiple**	**Cacti 0.5, 0.6-0.6.8**	**Several vulnerabilities exist: a vulnerability exists because user input is not checked when performing the rrdtool 'graph' command, which could let a malicious user execute arbitrary commands; a vulnerability exists because the 'config.php' file is world-readable, which could let a malicious user take over the database; and a vulnerability exists because path checking is not performed when users enter operating system commands in the Data Input field, which could let a malicious user obtain unauthorized access.** ***Note: The malicious user must have administrative access to exploit some of these vulnerabilities.***	***Upgrade available at:*** **http://www.raxnet.net/downloads/cacti-0.6.8a.tar.gz** ***Debian:*** **http://security.debian.org/pool/updates/main/c/cacti/**	**Cacti Multiple Vulnerabil-ities**	**Medium High** **(High if arbitrary code is executed)**	**Bug discussed in newsgroups and websites. The 'graphp' command vulnerability can be exploited via a web browser. There is not exploit required for the 'config.php' file and path checking vulnerabil-ities.**

[66] UkR Security Team Advisory, September 14, 2002.
[67] Debian Security Advisory, DSA-166-1, September 13, 2002.
[68] Bugtraq, September 3, 2002.
[69] Debian Security Advisory, DSA 164-1, September 10, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
RTFM[70]	Unix	ssldump 0.9 b2, 0.9 b1	Several vulnerabilities exist: a buffer overflow vulnerability exists in the decryption of malformed RSA keys, which could let a remote malicious user execute arbitrary code if the victim is running ssldump in "decryption" mode at the time of the attack; and a buffer underflow vulnerability exists when a SSLv2 'Challenge' value is copied, which could let a malicious user completely compromise the host.	Upgrade available at: http://www.rtfm.com/ssldump/ssldump-0.9b3.tar.gz	ssldump Buffer Overflow/ Underflow	**High**	Bug discussed in newsgroups and websites.
Savant[71]	Windows	Savant Webserver 3.1 & prior	A buffer overflow vulnerability exists when a GET request is sent that contains a URL of approx. 291 characters or more, which could let a remote malicious user execute arbitrary instructions.	No workaround or patch available at time of publishing.	Savant Webserver Buffer Overflow CVE Name: CAN-2002-1120	**High**	Bug discussed in newsgroups and websites. Proof of Concept has been published.
Savant[72]	Windows	Savant Webserver 3.1	Several vulnerabilities exist: a buffer overflow vulnerability exists in the 'cgitest.exe' file, which could let a malicious user cause a Denial of Service and potentially execute arbitrary code; a Denial of Service vulnerability exists when a malicious user sends a negative integer in the Content-Length value; and a vulnerability exists when a hexadecimal URL encoded "space" (%20) or "dot" (%2e) is appended to a request for a protected file or folder, which could let a remote malicious user bypass protection and obtain sensitive information.	No workaround or patch available at time of publishing.	Savant Webserver Multiple Vulnerabilities	Low/ Medium/ **High** **(Medium if sensitive informa-tion is obtained and High if arbitrary code is executed)**	Bug discussed in newsgroups and websites. There is no exploit code required.
SGI[73]	Unix	IRIX 6.5-6.5.14	A vulnerability exists due to insecure umask values for the root user, which could let a malicious user obtain sensitive information.	Upgrade to IRIX 6.5.15 or later available at: http://support.sgi.com/colls/patches/tools/relstream/index.html	IRIX Coredump Umask	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[70] Securiteam, September 12, 2002.
[71] Foundstone Inc. Advisory, 091002-SVWS, September 10, 2002.
[72] PivX Security Advisory, September 13, 2002.
[73] SGI Security Advisory, 20020902-01-I, September 18, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Squirrel Mail[74]	Unix	Squirrel Mail 1.2.7	Multiple Cross-Site scripting vulnerabilities exist in various PHP scripts because user input is not properly sanitized, which could let a malicious user execute arbitrary HTML and script code.	Upgrade available at: http://prdownloads.sf.net/squirrelmail/squirrelmail-1.2.8.tar.gz	SquirrelMail Multiple Cross Site Scripting	High	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.
Sun Micro-systems, Inc.[75]	Unix	Cobalt Control Station 4100CS, Cobalt Qube3 4000WG, Qube3 w/ Caching & RAID 4100WG, Qube3 w/Caching 4010WG, RaQ XTR 3500R, RaQ4 3001R, RaQ4 RAID 3100R	A vulnerability exists in /usr/lib/authenticate, which could let a malicious user obtain root privileges.	No workaround or patch available at time of publishing.	RaQ authenticate Root Privilege Escalation	High	Bug discussed in newsgroups and websites.
Sun Micro-systems, Inc.[76]	Unix	Solaris 8.0, 8.0_x86	A vulnerability exists in the asppppls(1M) utility because insecure temporary files are created with root privileges, which could let a malicious user obtain root privileges.	Patch available at: http://sunsolve.sun.com/pub-cgi/findPatch.pl?patchId=111299&rev=04	Sun Solaris ASPPPLS Insecure Temporary File Creation	High	Bug discussed in newsgroups and websites.
SuSE[77]	Unix	XFree86 X11R6 4.2.0	A vulnerability exists in the libX11.so library because it fails to disable the variable when the process is setuid, which could let a malicious user execute arbitrary code.	Update available at: ftp://ftp.suse.com/pub/suse/	XFree86 libX11.so Local Privilege Escalation	High	Bug discussed in newsgroups and websites. There is no exploit code required.
SWS[78]	Unix	Simple Web Server 0.0.4, 0.0.3, 0.1.0	A remote Denial of Service vulnerability exists when a malicious user sends a request that doesn't end with a newline.	Upgrade available at: http://www.linuxprogramlama.com/sws_web_server-0.1.1.tar.gz	Simple Web Server Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Symantec[79]	Windows 98/ME/NT 3.5/4.0/2000	Norton AntiVirus 2001	A Denial of Service vulnerability exists if a malicious user appends the e-mail client's POP3 username with several "/localhost" entries.	No workaround or patch available at time of publishing.	Norton Antivirus 2001 Poproxy Username Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.

[74] Bugtraq, September 19, 2002.
[75] Sun(sm) Alert Notification, 46988, September 10, 2002.
[76] Sun(sm) Alert Notification, 46903, September 11, 2002.
[77] SuSE Security Announcement, SuSE-SA:2002:032, September 18, 2002.
[78] Bugtraq, September 3, 2002.
[79] Securiteam, September 12, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Tolis Group[80]	Unix	BRU 17.0 Linux	A race condition vulnerability exists because the existence of temporary files is not properly checked before execution, which could let a malicious user overwrite root-owned files.	No workaround or patch available at time of publishing.	BRU Race Condition	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Trend Micro Inc.[81]	Windows, Unix	InterScan VirusWall 3.52, InterScan VirusWall (Linux) 3.6	Several vulnerabilities exist: a vulnerability exists because support for HTTP 1.1 Transfer-Encoding is not included, which could let a malicious user bypass scanning procedures; and a vulnerability exists because support for HTTP 1.0 gzip Content-Encoding is not included, which could let a malicious user bypass scanning procedures.	TrendMicro has been contacted and has said that InterScan VirusWall 5 will properly support HTTP 1.1 Transfer-Encoding. Until the time of it's release it is advised to use an alternative method for file integrity checking. It is possible to disable HTTP 1.1 in some web clients (such as Internet Explorer).	InterScan VirusWall HTTP 1.1 Transfer-Encoding & Content Encoding Bypass	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Ultimate PHP Board[82]	Multiple	Ultimate PHP Board 1.0, 1.0 b	A vulnerability exists due to insufficient user validation, which could let a malicious user obtain administrative privileges.	Upgrade available at: www.webrc.ca/php/upb.php	Ultimate PHP Board Unauthorized Administrative Access	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Veritas Software[83]	Windows NT 4.0/2000, Unix	Cluster Server 1.2 NT, 1.3 Solaris, 1.3 HPUX, 1.3	A vulnerability exists which could let a remote malicious user obtain root access.	Patches are available for VCS on the HP-UX and Solaris platforms at: http://ftp.support.veritas.com/pub/support/products/ClusterServer_UNIX/vcs.130-patch03_239344.tar.Z and ftp://ftp.veritas.com/pub/products/hp.vcs.131-patch03.tar.gz.y A version of Veritas Cluster Server containing the fix for Windows NT may be obtained by contacting a sales representative.	Veritas Cluster Server Root Compromise	**High**	Bug discussed in newsgroups and websites.
WoltLab GbR[84]	Unix	Burning Board 2.0 RC1, 2.0 beta 3-5	A SQL injection vulnerability exists due to insufficient santization of parameters handled by the 'board.php' script, which could let a remote malicious user corrupt the database and obtain administrative privileges.	Upgrade to the latest version of WoltLab Burning Board (2.0 RC 2 or later), when it becomes available from the WoltLab Web site. http://www.woltlab.info/en/forum/	Burning Board Board.PHP SQL Injection	Medium/ **High** **(High if adminis-trative access can be obtained)**	Bug discussed in newsgroups and websites. Exploit has been published.

[80] Bugtraq, September 13, 2002.
[81] Securiteam, September 12, 2002.
[82] SecurityFocus, September 6, 2002.
[83] SecurityTracker, September 9, 2002.
[84] Bugtraq, September 8, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Wordtrans [85, 86]	Unix	Wordtrans-web 1.0 beta-2-2.4, 1.1 pre8	A vulnerability exists in the 'wordtrans.php' script due to improper validation of input parameters, which could let a remote malicious user execute arbitrary code.	**Debian:** http://packages.debian.org/unstable/text/wordtrans-web.html **RedHat:** ftp://updates.redhat.com/	Wordtrans-web Remote Command Execution CVE Name: CAN-2002-0837	**High**	Bug discussed in newsgroups and websites.
Xbreaky[87]	Unix	Xbreaky .3, .4	A symbolic link vulnerability exists, which could let a malicious user corrupt arbitrary system files and possibly obtain elevated privileges.	Upgrade available at: http://xbreaky.sourceforge.net/download.html	Xbreaky Symbolic Link	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

Medium – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. *DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.*

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between September 5 and September 20, 2002, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing**. During this period, 43 scripts, programs, and net-news messages containing holes or exploits were identified. *Note: At times, scripts/techniques may contain names or content that may be considered offensive.*

Date of Script (Reverse Chronological Order)	Script Name	Script Description
September 20, 2002	**Trillian-privmsg.c**	**Script which exploits the Trillian IRC PRIVMSG Buffer Overflow vulnerability.**

[85] Guardent Client Advisory, September 6, 2002.
[86] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:188-08, September 9, 2002.
[87] Bugtraq, September 12, 2002.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
September 20, 2002	**Trillident.C**	**Script which exploits the Trillian IRC PRIVMSG Buffer Overflow vulnerability.**
September 20, 2002	John-1.6.32.tar.gz	A fast password cracker, currently available for many flavors of Unix (11 are officially supported, not counting different architectures), DOS, Win32, and BeOS.
September 20, 2002	Aimsniff-0.5.tar.gz	A utility for monitoring and archiving AOL Instant Messenger messages across a network which has the ability to do a live dump (actively sniff the network) or read a PCAP file and parse the file for IM messages.
September 20, 2002	M6.3-beta2-linux-bin-x86.tar.gz	The Mad Mass Scanner combines 12 remote exploits with Teso's telnetfp and exploits Bind, LPD, wu-ftp, sshd, telnetd, pop3, OpenSSL, and some RPC services.
September 19, 2002	Adore-0.42.tgz	A Linux LKM based rootkit for Linux v2.[24] that features smart PROMISC flag hiding, persistent file and directory hiding (still hidden after reboot), process-hiding, netstat hiding, rootshell-backdoor, and an uninstall routine.
September 19, 2002	Cisco-vpn-5000-lnx.c	Script which exploits the VPN 5000 Client Buffer Overflow Vulnerabilities.
September 19, 2002	Es-cisco-vpn.c	Script which exploits the VPN 5000 Client Buffer Overflow close_tunnel binary vulnerability.
September 19, 2002	**K3.c**	**Proof of Concept exploit ATFTP Get File Local Buffer Overflow vulnerability.**
September 19, 2002	**Netric_atftp_exploit.c**	**Script which exploits the ATFTP Get File Local Buffer Overflow vulnerability.**
September 18, 2002	**Free-apache.txt**	**FreeBSD Apache exploit based on apache-worm.c.**
September 18, 2002	Ohmy-another-efs.c	Efstool local root exploit which works against RedHat 7.3.
September 18, 2002	**Trillian-ident.c**	**Script which exploit the Trillian Identd Buffer Overflow vulnerability.**
September 18, 2002	Tru64_dxterm.pl	Perl script which exploits the Tru64/OSF1 DXTerm Buffer Overflow vulnerability.
September 17, 2002	Fv.txt	Finding Vulnerabilities explains the auditing of C source code to find application exploits and includes a practical example of how to hack an IDS that was coded for a website.
September 17, 2002	Hao_lconfmdk.c	Script which exploits the Linuxconf Mandrake vulnerability.
September 17, 2002	Idefense.libkvm.txt	Exploit information for the FreeBSD Ports libkvm Vulnerabilities.
September 17, 2002	**Openssl-too-open.tar.gz**	**Exploit for the Apache/mod_ssl KEY_ARG overflow vulnerability.**
September 16, 2002	**Netric-adv010.txt**	**Exploit technique for the ATFTP Get File Local Buffer Overflow vulnerability.**
September 15, 2002	**Bugtraqworm.tgz**	**This file contains the binaries and source code for the current Apache worm that affects multiple versions of Linux. It exploits an OpenSSL buffer overflow to run a shell on the remote system and also contains the ability to perform a DDoS attack.**
September 14, 2002	**Planetweb-ex.pl**	**Script which exploits the PlanetWeb Long GET Request Buffer Overflow vulnerability.**
September 13, 2002	**Ssldump-0.9b3.Tar.Gz**	**An SSLv3/TLS network protocol analyzer that identifies TCP connections on the chosen network interface and attempts to interpret them as SSLv3/TLS traffic.**
September 13, 2002	Nessus-1.2.5.tar.gz	A free, up-to-date, and full featured remote security scanner for Linux, BSD, Solaris and some other systems that is multithreaded, plugin-based, has a nice GTK interface, and currently performs over 920 remote security checks.
September 12, 2002	**Sx-slap.pl**	**Perl script which exploits the Savant Webserver Buffer Overflow vulnerability.**

Date of Script (Reverse Chronological Order)	Script Name	Script Description
September 12, 2002	Cdpsniffer-v1.0.tar.gz	A Perl Cisco discovery protocol (CDP) decoding sniffer that sniffs the network traffic, picks out the CDP packets and prints out the decoded protocol contents.
September 11, 2002	Autolinuxconf.tgz	Script which exploits the Mandrake Linuxconf vulnerability.
September 11, 2002	Coudrape.c	Script which exploits the Linux Efstool local root vulnerability.
September 11, 2002	Efstool.pl	Script which exploits the Linux Efstool local root vulnerability.
September 11, 2002	Newtcp.htm	Strange Attractors and TCP/IP Sequence Number Analysis includes 3D pictures of the sequence number distribution for several OS's and analyzes the predictability of each.
September 11, 2002	Targets.319	List of targets for the x2 remote crc32 ssh exploit which contains 319 entries.
September 10, 2002	Efstool.txt	Exploit for the Efstool local root vulnerability.
September 10, 2002	**Fs-091002-svws**	**Proof of Concept code for the Savant Web Server buffer overflow vulnerability.**
September 10, 2002	Tru64_dtaction	Proof of Concept local root exploit for dtaction on the HP/Compaq Tru64 Operating System.
September 10, 2002	Tru64_dtprintinfo	Proof of Concept local root exploit for dtprintinfo on the HP/Compaq Tru64 Operating System.
September 10, 2002	Tru64_dtterm	Proof of Concept local root exploit for dtterm on the HP/Compaq Tru64 Operating System.
September 10, 2002	Tru64_dxterm	Proof of Concept local root exploit for dxterm on the HP/Compaq Tru64 Operating System.
September 10, 2002	Tru64_nlspath	Proof of Concept local root exploit written in Perl for NLSPATH overflow on the HP/Compaq Tru64 Operating System.
September 10, 2002	Tru64_su	Proof of Concept local root exploit for su on the HP/Compaq Tru64 Operating System vulnerability.
September 10, 2002	Tru64_xkb	Proof of Concept local root exploit for _XKB_CHARSET vulnerability on the HP/Compaq Tru64 Operating System.
September 9, 2002	**Test-crash.zip**	**Exploit for the Outlook Express Link Denial of Service vulnerability.**
September 9, 2002	**Trillian-ini-decrypt.c**	**Script which exploits the Trillian Weak Password Encryption vulnerability.**
September 8, 2002	Create.c	Script which exploits the Multiple Vendor Zero Width GIF Image Files vulnerability.
September 5, 2002	Swsnewline-ex.c	Script which exploits the Simple Web Server Remote Denial of Service vulnerability.

Trends

- **The CERT/CC has received reports of self-propagating malicious code that exploits a known buffer overrun vulnerability in the Secure Sockets Layer 2.0 (SSLv2) handshake process in OpenSSL. This malicious code has been referred to as Apache/mod_ssl worm, linux.slapper.worm, and bugtraq.c worm. For more information see CERT® Advisory CA-2002-27, located at: http://www.cert.org/advisories/CA-2002-27.html. Please ensure that you've applied the appropriate patch. For more information regarding the virus, please see Virus Section.**
- **Statistical weaknesses exist in TCP/IP Initial Sequence Numbers. For more information, see CERT® Advisory CA-2001-09, located at: http://www.cert.org/advisories/CA-2001-09.html.**
- **The Microsoft Product Support Services (PSS) Security Team has issued an alert regarding an increased level of hacking activity. These hacking attempts show similar symptoms and behaviors involving the detection of Trojans such as Backdoor.IRC.Flood and its variants, and the modification of the security policy on domain controllers.**

- **Web CGI exploits and Microsoft vulnerabilities continue to be two of the more frequent ways which external malicious sources conduct their probes in their attempt to gain access to networks.**
- **According to data compiled by its regional Global Command Centers (GCCs), which monitor and protect client networks from cyber-attacks, there has been a surge in cyber-attacks originating from Malaysia over the last quarter. The majority of these attacks were mainly Apache exploit attempts to execute arbitrary codes, which could lead to possible Denial-of-Service (DoS) attacks.**
- **The Common Desktop Environment (CDE) ToolTalk RPC database server contains a buffer overflow vulnerability that could allow a remote malicious user to execute arbitrary code or cause a denial of service. For more information see CERT® Advisory CA-2002-26, located at: http://www.cert.org/advisories/CA-2002-26.html.**
- **There has been an increase in Distributed Denial of Service (DDoS) attacks reported in the first seven months of 2002 over the number of DDoS attacks last year.**
- **The National Infrastructure Protection Center (NIPC) has issued an advisory to heighten the awareness of multiple buffer overflows in OpenSSL (Open Secure Sockets Layer). For more information, see NIPC Advisory 02-006, located at: http://www.nipc.gov/warnings/advisories/2002/02-006.htm.**

Viruses

The following virus descriptions encompass new viruses and variations of previously encountered viruses that have been discovered in the last two weeks. The viruses are listed alphabetically by their common name. While these viruses might not all be in wide circulation, it is highly recommended that users update anti-virus programs as often as updates become available. *NOTE: At times, viruses may contain names or content that may be considered offensive.*

BAT_INA.A (Batch File Worm): This destructive mass-mailing worm spreads via IRC and the peer-to-peer network of KaZaA, a file-sharing application. It can update itself via the Internet using the File Transfer Protocol (FTP). It arrives in an e-mail through Microsoft outlook with the following details:

- Subject: hehe, isn't that fascinating...
- Message Body: ... I just want to say something to the attachment: It is the first ever batch virus that is able to update itself via the Internet! Hehe, you don't have to execute it (if you don't want to ;), but if you understand a bit batch, look at it, it's really interesting!
- Attachment: BAT.INA.

ELF_SLAPPER.A (Aliases: Linux/Slapper.worm Linux.Slapper.Worm, Linux/Slapper-A, Apache/mod_ssl Worm,) (Linux Worm): This worm has been reported in the wild. The worm tries to exploit a buffer overflow vulnerability in the OpenSSL component of SSL-enabled Apache web servers. Once active, the worm can be used as a backdoor to start up a range of Denial of Service attacks. Linux/Slapper-A spreads between systems via TCP port 443 (SSL). Before connecting to this port, the worm connects to TCP port 80 (HTTP) in order to try to customize its attack for specific Apache versions. If a web server other than Apache (or which identifies itself as other than Apache) is found, the worm will not attempt to infect. The worm looks for:

- Red Hat running Apache 1.3.6, 1.3.9, 1.3.12, 1.3.19, 1.3.20, 1.3.22, 1.3.23, and 1.3.26
- SuSE running Apache 1.3.12, 1.3.17, 1.3.19, 1.3.20, 1.3.23
- Mandrake running Apache 1.3.14, 1.3.19, 1.3.20, 1.3.23
- Slackware running Apache 1.3.26
- Debian running Apache 1.3.26
- Gentoo running any version of Apache.

If the system distribution or Apache version cannot be determined, the worm assumes Red Hat running Apache 1.3.23. Linux/Slapper-A connects via TCP port 443 (SSL) and tries to launch a shell (/bin/sh) on the remote system by exploiting a buffer overflow. The flaw in OpenSSL that allows Linux/Slapper-A to spread was announced and fixed in an OpenSSL Security Advisory of 30 July 2002. If Linux/Slapper-A

successfully breaks into its victim, the worm injects a shell script into the remote shell it has launched. The shell script contains a uuencoded copy of the worm's own source code. The script decodes this source code into the file /tmp/.bugtraq.c, compiles it using gcc into the executable file /tmp/.bugtraq and then executes it. A daemon process called .bugtraq will be visible on infected computers. *Note that the Linux/Slapper-A worm depends on the presence of the gcc compiler on victim computers, and also requires that the compiler be executable by the Apache user.* Once active, Linux/Slapper-A opens up a backdoor that can be contacted via UDP port 2002. The backdoor is intended to allow a range of attacks to be initiated from infected computers, such as: executing arbitrary commands; creating TCP floods; creating DNS floods and searching for e-mail addresses on disk.

ELF_SLAPPER.B (Linux Worm): This Linux malware is a C source code that is freely distributed on the Internet. When compiled, it can be used as a malicious tool against systems using FreeBSD 4.5 Apache 1.3.20-24. This variant of the worm, ELF_SLAPPER.A, uses a known vulnerability, which allows an attacker to be connected to the system using a shell on TCP port 30464. From there, other exploits can be used to access the root.

ELF_SLAPPER.C (Linux Worm): This ELF malware is a C source code that is freely distributed in the Internet. This Linux Trojan is a remote exploit for the KEY_ARG overflow in OpenSSL 0.9.6d and older. It gives an attacker remote shell, with the privileges of the server process, nobody, when used on Apache and root when used on other servers. This malware includes an OpenSSL vulnerability scanner, which is more reliable than the RUS-CERT scanner and has detailed vulnerability analysis.

VBS_INA.A (Aliases: VBS/Worm.Variant.Worm, VBS-merj.gen, I-Worm.Arica, Bloodhound.VBS.worm) (Visual Basic Script Worm): This is a Visual Basic Script (VBScript) component of BAT_INA.A. It facilitates the propagation of BAT_INA.A via e-mail.

VBS/Nedal-A (Aliases: VBS.Melhack.B, VBS/Amalad.a, VBS.VBSWG.AS, VBS/Nedal, I-Worm.Melhack) (Visual Basic Script Worm): This worm arrives in an e-mail with the following subject line:

- Subject line: Osama Bin Laden Comes Back!

The e-mail content is in HTML and includes a Visual Basic script that uses ActiveX. This script will probably produce a security warning, recommending that you do not allow the ActiveX component to run. If you do not allow the ActiveX component to run, the e-mail will contain a message indicating that you need ActiveX enabled if you want to see this e-mail. If you allow the ActiveX component to run, VBS/Nedal-A will write a copy of the worm into the file C:\Windows\OsamaBinLaden.vbs. The e-mail will contain a message from Bin Laden. VBS/Nedal-A may drop the following three programs into the Windows folder:

- osama.exe, laden.exe and alta.exe.

This is an overwriting virus that targets all files with EXE extensions. On the 11th of September, Laden.exe will display a message box that reads "Today is 11 September! Do you remember this date?." Laden.exe will drop the file C:\Laden.bat. It is intended to delete all files in the Windows system folder and will also create the following registry entry:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Laden = "Laden.exe"

This Trojan may display a message box that reads "Prepare to sleep..." and then cause Windows to shutdown. The Trojan creates the following registry entry to run the Trojan whenever Windows is started:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\AltaWorm = "alta.exe"

VBS/Nedal-A may also drop the batch file C:\OsamaLaden.bat. This batch file Trojan will create many new folders on the infected computer and will attempt to overwrite files that have the extensions TXT, XLS, DOC, EXE, RTF, CAB, COM, AVI, GIF, BMP, JPG, JPEG, TIF and BAT in the My Documents and C:\Windows\Desktop folders. VBS/Nedal-A creates the following registry entries:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\OsamaBinLaden
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\OsamaLaden

These two values will run the worm and the dropped batch file, OsamaLaden.bat, when Windows starts up.

W32.Appix.Worm (Win32 Worm): This is a worm that attempts to spread across file-sharing networks such as KaZaA and eDonkey2000. The worm infects PHP and PHTML files by appending code that is

designed to infect other PHP, PHTML, HTM, and HTML files. It also uploads the W32.Appix.Worm to a client computer that visits the infected Web site. Also, W32.Appix.Worm contains it own SMTP client engine that permits it to replicate using e-mail. The e-mail may arrive with the following characteristics:

- Subject: test23
- Attachment: Test.scr

W32/Chet-A (Aliases: W32.Chet@mm, W32/Chet@MM, WORM_CHET.A, W32/Anniv911.A-mm) (Win32 Worm): This is an e-mail worm which spreads via Microsoft Outlook Express. The worm moves itself to the Windows system folder as SYNCHOST1.EXE and creates the following registry entry to run itself on system restart:

- HKCR\Software\Microsoft\Windows\CurrentVersion\Run\ICQ1 = "C:\<Windows>\<system>\SYNCHOST1.EXE"

E-mails arrive with the following characteristics:

- Subject line: All people!!
- Attached file: 11september.exe

W32/Chet-A also sends out a report e-mail via SMTP to a remote address. This e-mail contains a list of the victims' e-mail addresses. The worm also deletes the registry entry:

- HKCR\Software\Microsoft\Windows\CurrentVersion\RunOnce

W32.Depress@mm (Win32 Worm/File Infector): This is a mass-mailing worm that uses Microsoft Outlook to send itself to all contacts in the Microsoft Outlook Address Book. Several variants have been found. All variants are written in the Microsoft Visual Basic Programming Language. It may be compressed with UPX. The e-mail message is "Take a look at these files i found on the Internet!! They are way cool!" The subject and attachment vary.

W32.Duksten@mm (Aliases: PE_DUKSTEN.A, W32/Duksten) (Win32 Worm): This is a mass-mailing worm that uses its own SMTP engine to send itself to all contacts in the Windows Address Book. The e-mail message has the following characteristics:

- From:"ISP_Tecnico"skudo@iris.es
- Subject: NetsKudo,proteccion IP para Windows9x/Me/Nt/2000/XP
- Attachment: Skudo.zip

W32.Duksten@mm is also a file infector that randomly infects random Portable Executable (PE) files.

W32/Flat.5129 (Win32 Virus): This is a virus that affects platforms with the .NET Framework tool installed. Its main action consists of infecting Windows files with an EXE extension. W32/Flat.5129 is programmed in C# and has a size of 5,129 bytes.

W32/Flatei.5129 (Alias: Syra) (File Infector Virus): This is another virus that makes use of Microsoft's .NET architecture. Due to the uncommon system requirements and replicating environment, currently, the virus is unlikely to become widespread. The .NET architecture must be installed on Windows2000/XP in order for the virus to function. One executable in the current directory is infected. The virus accomplishes this by prepending the file with the virus code, and appending a 5 byte marker at the end of the file.

W32.HLLC.Happylow (Aliases: HLLC.HappyFlowers, W32.Walcomp) (Win32 Virus): This is a companion virus that encrypts all .exe files that reside in the same folder as the virus and renames them with a .wal extension. It then makes a copy of itself as the original file name. For example, the virus encrypts the file Calc.exe and renames it to Calc.wal. Then the virus copies itself as Calc.exe, so that when the infected Calc.exe is executed, the virus executes its routine. Finally, it decrypts the Calc.wal file and executes it to make it appear that Calc.exe has run normally.

W32.HLLP.Alpoor (Alias: W32.Alpoor.6144) (Win32 Virus): This is a simple prepender virus that is written in Visual Basic .NET. The virus will only work under Windows 2000 and Windows XP with the .NET framework installed. When it is executed, it finds .exe files that exist in the same folder as the virus and then displays a message. Finally it infects the first file that it finds that is not already infected. It infects by prepending the virus to the file.

W32.HLLP.Flate (Aliases: W32.Alcarys.H, W32/Flatei.5129, Win32.HLLP.Flat.5129, Win32.HLLP.Flatei) (Win32 Virus): This is a prepender virus that is written in C# to infect Win32 executable files. The virus functions only if .NET Framework is installed. When the virus is executed it displays the message, "::: prepending virus purely written in d flat :::."

W32.HLLW.Efno (Alias: W32.Efno.Worm) (Win32 Worm): This is a worm that attempts to spread using the popular KaZaA file-sharing program. The worm is written in Visual Basic, and therefore it requires Visual Basic runtime libraries (Msvbvm60.dll) to run. When this worm runs, it changes several KaZaA registry keys. This causes the worm to be accessible to other users on the KaZaA network. The worm spreads using the file name "Win XP SP1 cracker.exe." However, it is possible to change the file name to other names that may appeal to people. *NOTE: If KaZaA is not installed on the computer, this worm does nothing.*

W32.HLLW.Dax (Win32 Worm): This is a worm that spreads through open shares across the network. It attempts to replicate itself to that share as the file "Ordin Popescu.exe." In its functionality, W32.HLLW.Dax is similar to W32.HLLW.Qaz.A. When W32.HLLW.Dax runs, it copies itself as %system%\Rundlll.exe. The worm creates the value, "PowerManagement %system%\rundlll.exe," in the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that the worm starts when you start or restart Windows. After the worm has replicated, it notifies the client side using e-mail. The text of the e-mail message contains the IP address of the infected computer. The backdoor payload opens port 3256 and waits for a connection. This enables a malicious user to connect to and gain access to the infected computer. The worm contains code that permits it to enumerate all fixed drives on the infected computer, and then enumerate and delete all files on those drives. Also, the worm may drop the file C:\Test.com and modify the C:\Autoexec.bat file with a command that runs the Trojan. Next, the worm may restart the computer; the Trojan then runs and overwrites critical data on the first physical drive with garbage. This leads to complete data corruption on the drive.

W32/PacJoke (Win32 Virus): W32/PacJoke is joke program that can be exchanged through the P2P network KaZaA. It disguises itself by appearing as the video game Pac-Man. If executed, the worm renames the following files:

- C:\COMMAND.COM -> C:\VIRUS.EXE
- C:\WINDOWS\WIN.COM -> C:\WINDOWS\WIN.TXT
- C:\WINDOWS\COMMAND.COM -> C:\WINDOWS\MENU.TXT

Once W32/PacJoke the file is renamed. Pac2000 remains as an active process that allows it to continuously open and close the CD-ROM drive. It then tries to power down the operating system.

WM97/Spatch-B (Alias: Macro.Word97.Swatch.b) (Word 97 Macro Virus): This virus creates the non-viral file C:\Tmp.bas, which it uses to replicate. The virus should then delete this file.

WORM_BOOSTAP.A (Internet Worm): This worm runs every time an .EXE file is executed. It does not stop running unless the executed .EXE file is also closed. This worm also mass-mails copies of itself. It uses SMTP or Simple Mail Transfer Protocol to send e-mail and constructs its e-mail messages such that they are run automatically on the recipient system. The e-mail subject and attachment can be a combination of various names.

WORM_DELTAD.A (Aliases: I-Worm.Deltad, W32.Deltad.A@mm, Win32/Delta.D@mm) (Internet Worm): This mass-mailing worm modifies the Internet Explorer homepage, causing the browser to point to the Windows update site everytime it is opened. It also drops a Visual Basic Script file, VBS_DELTAD.A. This VBScript malware propagates this worm as an attachment in e-mail with the following details:

- Subject: SAP UPDATE
- Message body: All: Please update your system. DGSAP
- Attachment: WWW.DGSAP.DELTADG.COM.EXE

WORM_DULOAD.C (Aliases: Worm.P2P.Duload.c, Win32/HLLW.Duload) (Internet Worm): This worm propagates via the KaZaA peer-to-peer file sharing network. During analysis, this worm variably dropped and installed several backdoor programs. Upon execution, this worm drops a copy of itself in the Windows System directory as SYSTEMRESTORER.EXE. It then registers itself as a process and stays resident in memory. It also drops a random number of copies of itself in the Windows directory and the Windows system directory. For these copies, it uses random filenames of random lengths, but uses only numbers as characters for the filenames (e.g. 1234567.890, 69126912.1).

WORM_PEPEX.A (Aliases: Win32/PEPEX@mm, PEPEX) (Internet Worm): This worm propagates via e-mail using SMTP (Simple Mail Transfer Protocol) commands. It sends out an e-mail with the following format:

- From: "Microsoft" <information@microsoft.com>
- Reply To: "Microsoft" microsoft@microsoft.com
- Subject1: Hello
- Subject: Internet Explorer vulnerability patch
- Message Body: You will find all you need in the attachment.
- Attachment: Setup.exe

WORM_VODNI.A (Alias: I-Worm.Indovirus.A) (Internet Worm): This worm propagates using Microsoft Outlook, mIRC, network mapped drives and floppy drives. Upon execution, this worm copies itself to the root directory of drive C as _.EXE. Then, it creates the following registry entry below so that its copy is executed at every Windows startup:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices {Default} = _.exe

It adds the entry below to the WIN.INI file, also to load its copy at every windows startup:

[windows]
Load=_.exe

Next, it searches for files with the following extensions in all folders on the infected system: TXT, EXE, LNK, DOC, XLS, JPG, MP3, MPG, HTM, HTML, ASP, ZIP, and RAR. For every file that it finds, it drops a copy of itself in the same folder where the found file is located. The filename of the dropped file is taken from the found file plus any of the following extension names: EXE, SCR, or PIF. Aside from dropping copies of itself into all local folders, it also drops copies of itself to all network mapped drives and floppy drives. It then connects to the site http://www.ind&ltblocked&gtirus.net, which contains virus-related articles and binaries. This worm also sends out an infected e-mail, with itself as an attachment, to all addresses listed in the Microsoft Outlook contact list. It sends e-mail with a random subject, body, and attachment name. Next, it searches for MIRC.INI, which is used by the mIRC chat client. Once found, it inserts malicious script at the [script] section of the .INI file. The malicious script configures the chat client to send copies of this worm, via DCC, to all other users joining the same channel that the infected user is currently in. On the 1st day of any month, this worm configures the registry so that all .EXE files are associated to the Notepad application. For instance, if an .EXE file is executed, say CALC.EXE.exe, the .EXE file fails to run. Notepad is launched instead, with the binary content of CALC.EXE opened by the editor. It modifies the registry to:

- HKEY_CLASSES_ROOT\exefile\shell\open\command {Default} = "notepad.exe %1"

As part of its payload, this worm displays a message box with the text:

- WELCOME TO OUR NETWORK -Indonesian Virus Network-

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table includes Trojans discussed in the last six months, with new items added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. *Note: At times, Trojans may contain names or content that may be considered offensive.*

Trojan	Version	CyberNotes Issue #
AIM-Flood	N/A	CyberNotes-2002-16
Arial	N/A	CyberNotes-2002-08
Backdoor.Anakha	N/A	CyberNotes-2002-13
Backdoor.AntiLam	N/A	CyberNotes-2002-12
Backdoor.AntiLam.20	20	CyberNotes-2002-18
Backdoor.Assasin	N/A	CyberNotes-2002-14
Backdoor.Cabro	N/A	CyberNotes-2002-17
Backdoor.Cabrotor	N/A	CyberNotes-2002-18
Backdoor.Crat	N/A	CyberNotes-2002-12
Backdoor.Cyn	N/A	CyberNotes-2002-18
Backdoor.DarkFtp	**N/A**	**Current Issue**
Backdoor.Delf	N/A	CyberNotes-2002-16
Backdoor.Delf.B	B	CyberNotes-2002-16
Backdoor.Delf.C	C	CyberNotes-2002-17
Backdoor.Ducktoy	N/A	CyberNotes-2002-15
Backdoor.Easyserv	N/A	CyberNotes-2002-16
Backdoor.Evilbot	N/A	CyberNotes-2002-09
Backdoor.Expjan	N/A	CyberNotes-2002-18
Backdoor.Fearic	N/A	CyberNotes-2002-16
Backdoor.FTP_Bmail	N/A	CyberNotes-2002-12
Backdoor.FunFactory	**N/A**	**Current Issue**
Backdoor.G_Door.Client	N/A	CyberNotes-2002-05
Backdoor.GRM	N/A	CyberNotes-2002-13
Backdoor.GSpot	N/A	CyberNotes-2002-12
Backdoor.Helios	**N/A**	**Current Issue**
Backdoor.Kavar	N/A	CyberNotes-2002-16
Backdoor.Kryost	N/A	CyberNotes-2002-18
Backdoor.Laphex	N/A	CyberNotes-2002-18
Backdoor.Laphex.Client	N/A	CyberNotes-2002-18
Backdoor.Lastdoor	N/A	CyberNotes-2002-18
Backdoor.Latinus	N/A	CyberNotes-2002-12
Backdoor.Latinus.B	B	CyberNotes-2002-18
Backdoor.Miffice	N/A	CyberNotes-2002-18
Backdoor.Mirab	N/A	CyberNotes-2002-13
Backdoor.Mite	N/A	CyberNotes-2002-18
Backdoor.MLink	N/A	CyberNotes-2002-16
Backdoor.Ndad	N/A	CyberNotes-2002-17
Backdoor.NetControle	N/A	CyberNotes-2002-13
Backdoor.Nota	N/A	CyberNotes-2002-12
Backdoor.Omed.B	B	CyberNotes-2002-11
Backdoor.Optix.04	**N/A**	**Current Issue**
Backdoor.OptixPro.10	10	CyberNotes-2002-18
Backdoor.OptixPro.12	12	CyberNotes-2002-18
Backdoor.Osirdoor	N/A	CyberNotes-2002-17
Backdoor.Phoenix	**N/A**	**Current Issue**
Backdoor.Ptakks.B	N/A	CyberNotes-2002-18
Backdoor.RCServ	**N/A**	**Current Issue**

Trojan	Version	CyberNotes Issue #
Backdoor.RemoteNC	N/A	CyberNotes-2002-09
Backdoor.Robi	N/A	CyberNotes-2002-18
Backdoor.Sazo	N/A	CyberNotes-2002-13
Backdoor.Scanboot	N/A	CyberNotes-2002-17
Backdoor.Seamy	N/A	CyberNotes-2002-18
Backdoor.Sparta	N/A	CyberNotes-2002-13
Backdoor.Sparta.B	**N/A**	**Current Issue**
Backdoor.Tela	N/A	CyberNotes-2002-17
Backdoor.Theef	N/A	CyberNotes-2002-15
Backdoor.Tron	N/A	CyberNotes-2002-12
Backdoor.Ultor	N/A	CyberNotes-2002-13
Backdoor.WinShell	N/A	CyberNotes-2002-16
Backdoor.Y3KRat.15	N/A	CyberNotes-2002-17
Backdoor.Zenmaster	**N/A**	**Current Issue**
BackDoor-ABH	N/A	CyberNotes-2002-06
BackDoor-ABN	N/A	CyberNotes-2002-06
BackDoor-AKR	**N/A**	**Current Issue**
Banan.Trojan	N/A	CyberNotes-2002-15
Bck/Litmus.201	N/A	CyberNotes-2002-14
BDS/ConLoader	N/A	CyberNotes-2002-12
BDS/EHKSLogger	**N/A**	**Current Issue**
BDS/Osiris	N/A	CyberNotes-2002-06
BKDR_EMULBOX.A	N/A	CyberNotes-2002-10
BKDR_INTRUZZO.A	N/A	CyberNotes-2002-09
BKDR_LITMUS.C	N/A	CyberNotes-2002-09
BKDR_WARHOME.A	N/A	CyberNotes-2002-06
Bneo.Trojan	N/A	CyberNotes-2002-18
Cardst	N/A	CyberNotes-2002-17
Dewin	N/A	CyberNotes-2002-08
Downloader-W	N/A	CyberNotes-2002-08
FakeGina.Trojan	N/A	CyberNotes-2002-16
Fortnight	N/A	CyberNotes-2002-10
IIS.Beavuh-Exploit	N/A	CyberNotes-2002-17
IRC.kierz	N/A	CyberNotes-2002-16
IRC-Smev	N/A	CyberNotes-2002-08
Jekord	**N/A**	**Current Issue**
JS/NoClose	N/A	CyberNotes-2002-11
Liquid.Trojan	N/A	CyberNotes-2002-14
mIRC/Gif	N/A	CyberNotes-2002-08
Multidropper-CX	N/A	CyberNotes-2002-08
Netbus.160.Dropper	N/A	CyberNotes-2002-17
PWS-AOLFake	N/A	CyberNotes-2002-15
PWS-MSNCrack	N/A	CyberNotes-2002-18
PWS-MSNSteal	N/A	CyberNotes-2002-17
PWS-Ritter	N/A	CyberNotes-2002-16
PWSteal.Kaylo	N/A	CyberNotes-2002-17
PWSteal.Netsnake	N/A	CyberNotes-2002-17
PWSteal.Profman	N/A	CyberNotes-2002-17

Trojan	Version	CyberNotes Issue #
PWSteal.SoapSpy	N/A	CyberNotes-2002-18
QDel227	N/A	CyberNotes-2002-09
QDel234	N/A	CyberNotes-2002-11
RCServ	N/A	CyberNotes-2002-10
Reboot-R	N/A	CyberNotes-2002-18
StartPage-B	N/A	CyberNotes-2002-16
Swporta.Trojan	N/A	CyberNotes-2002-13
TR/EvilDX	**N/A**	**Current Issue**
TR/Win32.Rewin	N/A	CyberNotes-2002-12
Tr/WiNet	N/A	CyberNotes-2002-10
TR/Zirko	N/A	CyberNotes-2002-10
Trj/GhostGirl	**N/A**	**Current Issue**
Troj/Apher-A	N/A	CyberNotes-2002-17
Troj/Diablo	N/A	CyberNotes-2002-09
Troj/DSS-A	N/A	CyberNotes-2002-12
Troj/FireAnv-A	**N/A**	**Current Issue**
Troj/Flood-O	N/A	CyberNotes-2002-14
Troj/ICQBomb-A	N/A	CyberNotes-2002-05
Troj/Kbman	N/A	CyberNotes-2002-10
Troj/Momma-B	N/A	CyberNotes-2002-11
Troj/Ritter-A	N/A	CyberNotes-2002-17
Troj/Tobizan-A	N/A	CyberNotes-2002-16
Troj/Unreal-A	N/A	CyberNotes-2002-16
TROJ_DOAL.A	N/A	CyberNotes-2002-14
TROJ_JUNTADOR.B	N/A	CyberNotes-2002-06
TROJ_JUNTADOR.G	N/A	CyberNotes-2002-10
TROJ_OPENME.B	N/A	CyberNotes-2002-09
TROJ_SMALL.J	N/A	CyberNotes-2002-10
TROJ_SMBNUKE.A	N/A	CyberNotes-2002-18
TROJ_SQLSPIDA.B	N/A	CyberNotes-2002-11
TROJ_SUOMIA.A	N/A	CyberNotes-2002-18
TROJ_WORTRON.10B	N/A	CyberNotes-2002-12
Trojan.Adclicker	**N/A**	**Current Issue**
Trojan.Adnap	N/A	CyberNotes-2002-17
Trojan.Allclicks.A	N/A	CyberNotes-2002-13
Trojan.Avid	**N/A**	**Current Issue**
Trojan.Beway	N/A	CyberNotes-2002-15
Trojan.Crabox	N/A	CyberNotes-2002-17
Trojan.DiabKey	N/A	CyberNotes-2002-18
Trojan.Diskfil	**N/A**	**Current Issue**
Trojan.Fatkill	N/A	CyberNotes-2002-09
Trojan.IrcBounce	**N/A**	**Current Issue**
Trojan.Junnan	N/A	CyberNotes-2002-16
Trojan.Lovead	**N/A**	**Current Issue**
Trojan.Nullbot	**N/A**	**Current Issue**
Trojan.Portacopo:br	N/A	CyberNotes-2002-16
Trojan.Prova	N/A	CyberNotes-2002-10
Trojan.PSW.Ajim_bbs	**N/A**	**Current Issue**

Trojan	Version	CyberNotes Issue #
Trojan.PSW.CrazyBilets	N/A	CyberNotes-2002-12
Trojan.PSW.M2	N/A	CyberNotes-2002-13
Trojan.Starfi	N/A	CyberNotes-2002-16
Trojan.Win32.Filecoder	N/A	CyberNotes-2002-18
Trojan.Win32.MSNTrick	N/A	CyberNotes-2002-17
VBS.Lavra.B.Worm	**N/A**	**Current Issue**
VBS.Zevach	N/A	CyberNotes-2002-15
VBS_CHICK.B	N/A	CyberNotes-2002-07
W32.Alerta.Trojan	N/A	CyberNotes-2002-05
W32.Azak	N/A	CyberNotes-2002-16
W32.Cbomb	N/A	CyberNotes-2002-16
W32.Click	N/A	CyberNotes-2002-15
W32.Delalot.B.Trojan	N/A	CyberNotes-2002-06
W32.DSS.Trojan	N/A	CyberNotes-2002-09
W32.Estrella	N/A	CyberNotes-2002-13
W32.Evala.Worm	N/A	CyberNotes-2002-14
W32.IRCBot	N/A	CyberNotes-2002-14
W32.Kamil	N/A	CyberNotes-2002-16
W32.Kotef	N/A	CyberNotes-2002-16
W32.Libi	N/A	CyberNotes-2002-10
W32.Maldal.J	N/A	CyberNotes-2002-07
W32.Nuker.Winskill	N/A	CyberNotes-2002-15
W32.Tendoolf	N/A	CyberNotes-2002-09
W32.Wabbin	N/A	CyberNotes-2002-15
WbeCheck	N/A	CyberNotes-2002-09
Winshell	N/A	CyberNotes-2002-15

BackDoor-AKR: This is a remote access Trojan. When run, it copies itself to Windows system directory as internat.dic and Windows directory as, "notepad.jmp." It creates and modifies several registry keys to load itself at startup:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\windows=%Windows system path%internat.dic
- HKEY_CLASSES_ROOT\txtfile\shell\open\command\(Default)= %Windows path%notepad.jmp
- HKEY_CLASSES_ROOT\.dic\(Default)=exefile
- HKEY_CLASSES_ROOT\.jmp\(Default)=exe

It opens TCP port 3721 to allow a remote attacker to connect to the infected system and perform various tasks.

Backdoor.DarkFtp (Aliases: BKDR_DARKFTP, BackDoor-KE.svr): This is a backdoor Trojan horse that gives an attacker unauthorized access to an infected computer. By default, it opens port 6667 on the compromised computer. The compromised system is then controlled by commands transmitted over IRC.

Backdoor.FunFactory: This is a backdoor Trojan that allows unauthorized access to an infected computer. It also allows voice communication from the intruder to the user of the compromised computer. Backdoor.FunFactory is written in Delphi. Its client allows access to selectable IP addresses and selectable ports. It requires that certain commercial software packages be installed for it to run. These packages are:

- Agentsvr.exe (Microsoft Agent)
- Merlin.exe (a Microsoft Agent script helper and character)
- Spchapi.exe (Microsoft Speech API module)
- Tv_enua.exe (A text-to-speech module)

Backdoor.FunFactory does not create any registry keys or drop files other than the client program, which can be run from anywhere on the infected system. The client is placed on the target system rather than being downloaded or installed by another process. Client UI allows for creation of "custom" scripts for speech and voice contact.

Backdoor.Helios (Alias: Backdoor.Helios.12.d): This is a backdoor Trojan horse that gives an attacker unauthorized access to an infected computer. By default it opens port 3737 on the compromised computer. The Trojan attempts to disable some antivirus and firewall programs by terminating the active processes. It is written in Microsoft Visual Basic version 6. When Backdoor.Helios runs, it copies itself as %system%\Scanstartup.exe. The file has the read-only, system, and hidden attributes. The Trojan creates the value, "SCANSTRTUP %system%\Scanstartup.exe," in the registry keys:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices

so that the Trojan starts when you start or restart Windows. It also creates the value, "StubPath %system%\Scanstartup.exe," in the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\ActiveSetup\Installed Components

It notifies the client side using ICQ pager and opens port 3737. The Trojan attempts to kill numerous processes. The Trojan's functionality allows the malicious user to perform any of the following actions:

- Deliver system and network information to the malicious user, including login names and cached network passwords
- Print text, play media files, and open or close the CD-ROM drive
- Intercept confidential information by hooking keystrokes; intercepting information that appears on the screen and delivering it to the malicious user
- Force the computer to shut down, restart, or log off

Backdoor.Optix.04 (Aliases: Backdoor.Optix.04.d, BackDoor-RS): This is a backdoor Trojan that gives an attacker unauthorized access to an infected computer. By default it opens port 27379 on the compromised computer. This Trojan attempts to disable some antivirus and firewall programs by terminating processes. Backdoor.Optix.04 is a Delphi application, packed with ASPack v2.10. When Backdoor.Optix.04 runs, it displays this message, “missing plugin 49587349,” and copies itself as:

- %windir%\Olefiles\Yahoo updater.com
- %system%\Tapisvc.sys

The Trojan creates the following registry keys:

- HKEY_LOCAL_MACHINE\SOFTWARE\EES
- HKEY_LOCAL_MACHINE\Software\EES\OL0.4

The values created in these keys store internal configuration data in an encrypted form. Backdoor.Optix.04 creates the value, “Common Startup %windir%\olefiles,” in the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders

so that the Trojan starts when you start or restart Windows. After the Trojan is installed, it establishes a connection with the malicious user through a password-protected authorization. The commands allow the malicious user to perform any of the following actions:

- Deliver system and network information to the malicious user
- Manage the installation of the backdoor Trojan
- Download and execute files

Backdoor.Phoenix (Aliases: BackDoor-RV.svr, BKDR_PHOENIX.190, Troj/Bdoor-RV): This is a Backdoor Trojan that gives an attacker unauthorized access to an infected computer. When Backdoor.Phoenix runs, it drops itself as the following files:

- ~P2.exe (This file is created in the same folder as the Trojan.)
- %windir%\Ctwdm16.exe
- %windir%\Ctcheklv.exe
- %windir%\Ssdpcache.exe

The Trojan creates these values:

- Ctwdm16.exe %windir%\Ctwdm16.exe

- Ssdpcache.exe %windir%\Ssdpcache.exe /doc

in the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that the Trojan starts when you start or restart Windows. It creates the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Ph

and in that key it creates the value:

- InstallationDate <The Trojan installation date> For example: <Thursday 10 May 2001 - 11:28:24>

In addition, Backdoor.Phoenix creates the value:

- <path to the Trojan>\~P2.EXE %windows%\Ctwdm16.exe /del <path to the Trojan>\~P2.EXE

in the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

After the Trojan is installed, it notifies the client side through e-mail. It accepts commands from the remote client on port 7410. The commands allow the malicious user to perform any of the following actions:

- Deliver system and network information to the malicious user, including login names and cached network passwords
- Print texts, play media files, open or close the CD-ROM drive, and perform other annoying actions
- Manage the installation of the backdoor Trojan
- Download and execute files

Backdoor.RCServ (Alias: Backdoor.RCServ.c): This is a Backdoor Trojan that gives an attacker unauthorized access to an infected computer. By default it opens port 4128 on the compromised computer. Backdoor.RCServ is a Delphi application, packed with UPX v1.20.

Backdoor.Sparta.B (Aliases: Backdoor.Spartadoor.11.a, BKDR_SPARTA.11, BackDoor-AFC): This is a backdoor Trojan horse that gives an attacker unauthorized access to an infected computer. It is a variant of Backdoor.Sparta. By default it opens port 6969 on the compromised computer. When Backdoor.Sparta.B runs, it copies itself as %system%\Spfile\Norten.exe and creates the value, "Common Startup %system%\spfile\," in the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ User Shell Folders

so that the Trojan starts when you start or restart Windows. The Trojan attempts to disable some antivirus and firewall programs by terminating the active processes. The commands allow the malicious user to perform any of the following actions:

- Print texts, play media files, open or close the CD-ROM drive, and perform other annoying actions
- Manage the installation of the backdoor Trojan
- Download and execute files

Backdoor.Zenmaster (Aliases: Backdoor.Zenmaster.101, BKDR_ZENMASTER.A, PWS-Hooker.dr): This is a backdoor Trojan horse that gives an attacker unauthorized access to an infected computer. Backdoor.Zenmaster is a Visual C++ application, and is packed using UPX v1.20. When Backdoor.Zenmaster runs, it drops itself as %system%\Winfiles.exe. It then drops K_File.exe (5,632 bytes) into the same folder. This file is not malicious; it is used by the Trojan to terminate processes. The Trojan creates the value, "HKDevice %system%\Winfiles.exe," in the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that the Trojan starts when you start or restart Windows. Backdoor.Zenmaster retrieves connection details by enumerating RAS connections. The data that the Trojan obtains is used to authenticate its access to the remote access server. The Trojan then delivers the retrieved information to a Web site. Also, the data may be used to enumerate and terminate running processes.

BDS/EHKSLogger: This Trojan will potentially allow someone with malicious intent backdoor access to your computer. If executed, the Trojan adds the following files to the \windows\%system\ directory,

"YMUpdater.exe" (Key Logger application) and "EHKS2.HTM" (Log file). So that it gets run each time a user restart their computer the following registry key gets added:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run YMUpdater="c:\\windows\\system\\YMUpdater.exe

Jekord: This is written in Borland Delphi. When run on the victim machine, it copies itself as LOADWMGR.EXE in C:\ (NT/2000) or %WinDir% (Win9x). IMAGES.DLL is copied to C:\ (NT/2000) or %WinDir% (Win9x) and the following Registry key is hooked to run the file at startup:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "LoadWinMgr" = '%path%\loadwmgr.exe'

The Trojan reads through the victim's browser history files and cookie data. Strings within the Trojan suggest it attempts to mail information to the malicious user (extracted from browser history files perhaps?) via a public script library (on an Estonian web portal).

TR/EvilDX: This Trojan will potentially allow someone with malicious intent backdoor access to your computer. If executed, the Trojan copies itself to C:\autoexec.bat and in the C:\windows\system32\directx directory under the filename "dxdiag.exe."

Trj/GhostGirl: This is a Trojan that does not cause any damage to affected computers. It is written in Visual Basic 6. Its effects take place at random and they are more irritating than damaging:

- It displays a photograph on the screen.
- It opens and closes the CD-ROM tray.

Troj/FireAnv-A (Aliases: FireAnvil, Trojan.Win32.FireAnvil, FireAnvil application): This is a Trojan that attempts to overwrite the beginning of every file on the hard disk with the text "CzY CrAcKiNg CrUe! We CrACk EvErYtHiNg!." There have been reports that Troj/FireAnv-A has been distributed in a commercial product, but at the time of writing it is believed that this download has been replaced with a clean version.

Trojan.Adclicker: This is a Trojan horse that is designed to click on banner advertisements on certain Web pages. Most likely these Web pages belong to the author of the Trojan. When the Trojan runs, it creates a copy of itself in the %system% folder, and it may also add itself to a registry \Run key.

Trojan.Avid (Aliases: Flooder.Win32.Avid, Avid, TROJ_AVID.A, Troj/Cill): This is a malicious threat that steals locally saved America Online (AOL) Instant Messenger passwords, and sends them to a specific e-mail address. When Trojan.Avid runs, it searches for the registry key:

- HKEY_CURRENT_USER\Software\America Online\AOL Instant Messenger (TM)\CurrentVersion\Users

This registry key contains encrypted passwords for AOL Instant Messenger if you have saved them locally on the computer. Trojan.Avid inserts the passwords into the body of an e-mail message, and sends the message to, Poopdeck@jive.net, with a notation that it is from, Avid Poster!" The message subject is:

- I must inquire about my antique shat...passed down by loving grandmother!

It does this by using a form that it creates within an HTML page that is named C:\Fun.html.

Trojan.Diskfil (Aliases: Diskfill-C, Troj_Garlic.B): This is a Trojan horse that copies system files to the root of drive C many times until the drive is full. When Trojan.Diskfil runs, it displays a fake message and then makes numerous copies of these files:

- C:\Windows\Explorer.exe
- C:\Windows\System\User.exe
- C:\Windows\System\Kernel32.dll
- C:\Windows\Regedit.exe
- C:\Windows\Winhlp32.exe
- C:\Windows\Scanregw.exe

using various file names. The Trojan adds a number to the end of the file name for each subsequent copy and continues to do this until drive C is full.

Trojan.IrcBounce (Aliases: Trojan/Bounce, W32/Bounce): This is the detection for a collection of programs that a malicious user can use to conceal intrusion and obtain administrator-level access to Microsoft Windows environments. These programs can be used to attack Windows environments that:

- Have the default installation, in which the Administrator account has no password
- Use user names and passwords that are very common.

After it is installed into victim's system, it gives a remote attacker unobstructed access to the compromised computer.

Trojan.Lovead (Aliases: Trojan.W32.Loveadot.f , Adshow): This is a Trojan horse that is written in Microsoft Visual Basic 5. When Trojan.Lovead runs, it copies itself as C:\Windows\System\Sysgo.exe and creates a file named, "C:\Sysgo.bat." It then adds to the C:\Autoexec.bat file a command that refers to Sysgo.bat. When Sysgo.bat runs, it copies C:\Windows\System\Sysgo.exe to C:\Windows\StartMenu\Programs\Startup\F.exe. As a result, each time that you start the computer (Windows 95/98/ME only), Sysgo.bat, and the Trojan are executed. When the Trojan runs, if you open a Web browser and connect to the Internet, the Trojan attempts to connect to www.loveadot.com, search a particular Web site using the keyword "kcsmith," and then display the results. It is possible that the Trojan's author in an effort to make money for his site by having the infected computer "click" an advertising banner did this.

Trojan.Nullbot (Alias: W32/NullBot): This is an IRC Trojan that allows a malicious user to gain control of the infected computer. It is written in the Microsoft C programming language and may be compressed two times with UPX and ASPack. When Trojan.Nullbot runs, it copies itself as C:\%system%\System.exe and adds the value, "Microsoft IPC system.exe," to one of these registry keys:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices

so that it runs each time that you start Windows. The Trojan contains its own Internet Relay Chat (IRC) client. This allows the Trojan to connect to an IRC channel that was coded into the Trojan. Using the IRC channel, the Trojan listens for commands from the malicious user. The malicious user accesses the Trojan by using a password-protected authorization. The commands allow the malicious user to perform any of the following actions:

- Manage the installation of the backdoor
- Dynamically update the installed Trojan
- Uninstall itself
- Deliver system and network information to the malicious user
- Control the IRC client on the compromised computer
- Send the Trojan to other IRC channels in an attempt to compromise more computers
- Download and execute files
- Perform Denial of Service (DoS) attacks against a target that is defined by the malicious user

Trojan.PSW.Ajim_bbs (Alias: Trojan.PSW.Delf.ac): This is a password-stealing Trojan horse. The default file name for the Trojan is Setup.exe. The Trojan will also modify various default settings for Internet Explorer. When Trojan.PSW.Ajim_bbs runs, it creates a new copy of itself as "%windir%\Winupdate.exe and %windir%\System32\Internets.exe." It overwrites the existing %windir%\Winver.exe file with a copy of itself. It overwrites the original %windir%\Hosts file with its own special Hosts file. It creates Set.ini in the same folder as the folder from which the Trojan the was run for the first time. It also attempts to copy Set.ini into the %windir%\Desktop folder so that the file appears on the Windows desktop.

VBS.Lavra.B.Worm (Alias: VBS.Thambl): This is a Trojan horse that is written in Microsoft Visual Basic Script. It attempts to delete antivirus and personal firewall software. In an attempt to spread, it copies itself as numerous files to the shared folders of several file-sharing programs.